10/747,912

SN 11/24/03

LCD) and keyboard, the plug-in of FIG. 7 may be used. The device is essentially a ~~headset~~ handset including a smartcard reader, preferably with 2 biometric sensors, one for the voice and the other one for the fingerprint. This is a highly secured device, including a timestamped Private Key that is generally locally and linked to the biometric information. The smartcard used may be a payment card or any service card (i.e., SIM or 7816 size). Up to 5 or more smartcard may be read simultaneously.

5. Please amend the paragraph that begins line 6 of page 15 and ends line 12 of page 15 as follows:

SN 11/24/03

In the preferred configuration of this embodiment, the biometric ~~headset~~ handset includes a (cryptographic) processor to perform elliptic curves and random number generator. A dedicated ASIC/DSP sends and receives the DTMF/FSK signals. In addition to other advantages, the system can deliver a vocal instruction to the handset~~head-set~~ and receive the voice as a second biometric identification from the microphone of the headset. The device is battery operated with a backup. Other features include an atomic time clock and software that can be updated by way of a smartcard (SIM or 7816 size) javacard or DTMF/FSK. The amount of memory is optional. Policy (in encrypted XML) considerations may also be stored on the smartcard.

6. Please amend the paragraph that begins line 13 of page 15 and ends line 15 of page 15 as follows:

When the handset~~headset~~ is attached, the associated PDA, computer, or phone keyboard sends DTMF signals which are recognized by the device. PDA or phone screen can be updated thru a WAP application link to a vocal server.